

Office Action Summary	Application No.	Applicant(s)	
	10/566,206	QIAO ET AL.	
	Examiner	Art Unit	
	Christian LaForgia	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 25 January 2008.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-7 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1,2 and 4-7 is/are rejected.
 7) Claim(s) 3 is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 06 January 2007 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input checked="" type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. <u>mail'd w/OA</u> . |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____. | 6) <input type="checkbox"/> Other: _____. |

DETAILED ACTION

1. The amendment of 25 January 2008 has been noted and made of record.
2. Claims 1-7 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-7 have been considered but are moot in view of the new grounds of rejection.
4. See further rejections set forth below.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Corrigendum 1 to Recommendation H.248, hereinafter H.248, in view of U.S. Patent No. 7,089,211 B1 to Trostle et al., hereinafter Trostle. H.248 references RFC 2409, thereby incorporating it by reference. The Examiner will refer to RFC 2409 to show features not expressly stated in H.248. See MPEP § 2131.01.

7. Section 10 of H.248 sets forth an outline for claim 1. H.248 is a standard for interaction between media gateways and media gateway controllers. Section 10.1 specifically states that

[i]mplementations SHOULD use IKE [RFC2409] to permit robust keying options. Implementations employing IKE SHOULD support authentication with RSA signatures and RSA public key encryption.

Referring to RFC 2409, we learn that each party has their own key to validate digital signature as a means of authentication, most explicitly in Section 5, pages 8-20. H.248 also takes into session keys in section 10.3 on page 47.

8. H.248 does not show updating the encryption key when it has expired.

9. Trostle teaches the updating of session keys in response to normal expiration or other causes (column 10, lines 50-52).

10. It would have been obvious to one of ordinary skill in the art at the time the invention was made to update the session key when it expired, since Trostle states at column 10 lines 45-50 that key updates are vital to maintain the secure nature of the communication.

11. With regards to claim 5, RFC 2409 teaches that the algorithm used to generate a shared key by said Media Gateway Controller and said Media Gateway is different from the algorithm used to generate a digital signature by said Media Gateway Controller and said Media Gateway (section 5, pages 8-20).

12. With regards to claim 6, RFC 2409 teaches that a field/packet of an expanded protocol is used to transmit said parameter for generating a shared key and said digital signature (section 5, pages 8-20).

13. Regarding claim 7, H.248 discloses the use of session keys as discussed above. Session keys include a lifetime the key that is either time or the number of times said shared key can be used as noted by page 216 of Stallings.

14. Claims 2 and 4 rejected under 35 U.S.C. 103(a) as being unpatentable over H.248 and Trostle as applied to claim 1 above, and further in view of **Cryptography and Network Security**, by William Stallings, hereinafter Stallings.

15. Regarding claims 2 and 4, H.248 teaches generating a new shared key further comprises:

initiating a register signaling from said Media Gateway to said Media Gateway Controller to register, wherein said register signaling has a parameter for generating a shared key and a digital signature generated by said initial key (Section 10, pages 46-48); generating a shared key (i.e. session key) as discussed above. Furthermore, since H.248 discloses the use of session keys the lifetime of said shared key after said Media Gateway Controller has validated said Media Gateway with said initial key should be set as noted with respect to claim 7.

16. Neither H.248 and Trostle teach initiating a modification command from said Media Gateway Controller to said Media Gateway, wherein said modification command has a parameter for generating the shared key, a digital signature generated by said initial key and a lifetime of a shared key; and generating the shared key and setting up the lifetime of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key.

17. It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate a new shared key, since Stallings states at page 216 that the more frequently the session key are exchanged, the more secure they are, because the opponent has less ciphertext to work with for any given session key.

Allowable Subject Matter

18. Claim 3 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

19. The following is a statement of reasons for the indication of allowable subject matter: Claim 3 requires that a digital signature be attached to each call. The Examiner is unable to find any teaching of said feature as well as nothing that would render said limitation obvious. Therefore, claim 3 is objected to as containing allowable subject matter.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

21. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

24. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

clf